

QUE FAIRE DÈS L'ANNONCE DE LA CYBER-ATTAQUE ?

« image : Freepik.com »



Isoler le système d'information de la DGFIP

Dans un contexte de recrudescence, de sophistication de la menace et de nécessaire transformation numérique, la cybersécurité est plus que jamais un enjeu majeur pour les collectivités et établissements publics, régulièrement ciblées par les attaquants.

Communes, communautés de communes, conseils départementaux, conseils régionaux, hôpitaux.. La menace Cyber n'épargne plus aucune structure, pouvant entraîner de lourdes conséquences (interruption de service pendant plusieurs jours ou semaines, fuite de données etc.) tant pour l'entité qu'elle représente que pour ses parties prenantes (administrations, autres administrations, État...).

Un des enjeux est de réagir rapidement afin de stopper tous les échanges entre le système d'information attaque et celui de la DGFIP.

CYBER ATTAQUE

**BLOQUER LES FLUX
EN PROVENANCE DE
L'ORDONNATEUR**

**STOPPER LES ACCÈS
DES RÉGISSEURS AU
PIGP**

**PRÉVENIR LES
INTERLOCUTEURS
COMPÉTENTS AU
SEIN DE LA DGFIP**

> Bloquer les flux en provenance du système d'information de l'ordonnateur

[Être prévenu

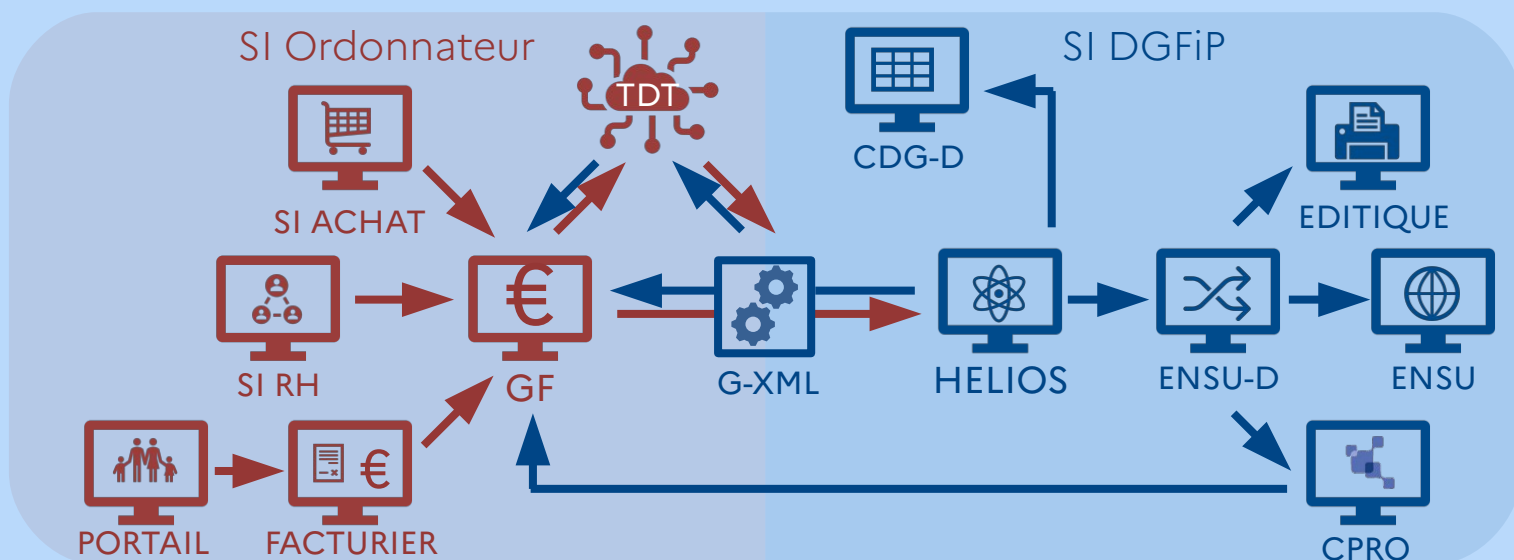
Le comptable public doit être informé par l'ordonnateur dès la connaissance de l'attaque. Les échanges informatiques doivent être stoppés. L'ordonnateur doit stopper les émissions de données à destination du comptable, informer le tiers de télétransmission si la collectivité ou l'établissement a recours à un tel service. Le comptable stoppe la réception des flux.

[Cartographier

Le comptable doit obtenir de l'ordonnateur une cartographie du système d'information impacté, afin de connaître le périmètre des budgets pour lesquels les échanges doivent être interrompus, et de prévoir comment assurer la suite et la continuité de service.

- Il convient de savoir quels sont les logiciels en place et s'ils sont touchés par l'attaque (Gestion financière, Logiciel(s) facturier(s), Gestion RH, SI Achat ...)
- L'ordonnateur et son DSI recensent ensuite les collectivités ou toutes entités (syndicats, associations foncières..) utilisant également ces outils et la même infrastructure informatique ;
- Le comptable public doit bloquer tous les flux informatiques (PESV2 et pièces justificatives) entrants et sortants de la collectivité (et des collectivités utilisant la même infrastructure informatique) tant que l'incident n'est pas terminé ; **Pour cela il est nécessaire de supprimer dans Hélios les paramétrages d'échanges de flux (Échanges Flux PES).**
- **Si la collectivité utilise les API de la DGFIP**, il est nécessaire de le préciser afin de faire supprimer les jetons d'accès.

PRINCIPAUX ÉCHANGES ORDONNATEUR - COMPTABLE



[Stopper les échanges HELIOS

Dans HELIOS : le comptable public doit supprimer les échanges de données Aller et Retour. Il est nécessaire de procéder dans l'ordre suivant :

- Supprimer dans un premier temps l'ensemble des paramètres ordonnateur « retour »
- Puis dans un second temps l'ensemble des paramètres ordonnateur « aller ».
- Conserver une vue des paramètres pour les rétablir le moment venu (Captures d'écran).
- Cette action doit être réalisée pour tous les budgets de la collectivité = budgets annexes, rattachés, principaux ou utilisant les infrastructures informatiques de la collectivité AFR, syndicats...

Paramétrage	Archives	Assistance
CHD		
Catégories Inventaire		
Domaines		Détail
Echanges PES		

Paramètres Ordonnateur Multi-budgets ☐

Aller	Action	Retour	Action
		Protocole PES retour V2	
		Périodicité Quotidien	
Protocole Divers	Modif	Mode de gestion	Modif
		Mode de transfert	

PARAMÉTRAGE—ECHANGES PES—SELECTION DES PROTOCOLES RETOUR 1

Sélection détaillée des protocoles Retour Ordonnateur

Type de message	Protocole	Périodicité	Mode de gestion	Mode de transfert	Date de démarrage	Action
Mandat PES V2-S	PES retour V2	Quotidien			19/11/2016	Suppr

PARAMÉTRAGE—ECHANGES PES—LISTE DES PARAMÈTRES D'ÉCHANGE 1

Sélection d'un budget collectivité ou d'une collectivité

Budget Collectivité* (valeurs) 10000 - Multi-budgets ☐ Filter

Liste des budgets collectivité (total 1 budgets)

Budgets	Ordonnateurs	Activation	Affich/Action
		Début	Fin
10000 divers	divers	23/01/2019	01/01/2099

PARAMÉTRAGE—ECHANGES PES—SELECTION DES PROTOCOLES ALLER 1

10000 - VILLE DE PARIS

Sélection globale des protocoles Aller Ordonnateur

Protocole PES aller V2 signé Actualiser

Sélection détaillée des protocoles Aller Ordonnateur

Type de message	Protocole	Action
Bordereau mandats ordinaires	PES aller V2 signé	Suppr
Bordereau mandats annulation	PES aller V2 signé	Suppr
Bordereau ordres paiement ord	PES aller V2 signé	Suppr
Bordereau mandats émis d'off	PES aller V2 signé	Suppr
Bordereau titres ordinaires	PES aller V2 signé	Suppr
Bordereau titres annulation	PES aller V2 signé	Suppr
Bordereau ordres recette ord	PES aller V2 signé	Suppr
Bordereau titres émis d'offi	PES aller V2 signé	Suppr
Bordereau Ordre de recette m	PES aller V2 signé	Suppr

> Suppression des paramètres Retour

> Suppression des paramètres Aller



En cas de message d'erreur lors de la démarche de blocage des flux, il est possible de paramétrer un «mauvais protocole» type Indigo inventaire à la place du "PES V2 signé", bloquant ainsi l'intégration des flux. Une fois les changements de paramètres validés, il est nécessaire de sortir de la transaction et de consulter à nouveau la bonne prise en compte des modifications.

[Traitement des flux en attente en bannette

Les flux non traités et présents en bannette pour les budgets attaqués peuvent avoir été transmis à Hélios tandis que l'attaque pouvait être en cours. Les données des flux PESV2 peuvent avoir été corrompues (modifiées) et les pièces justificatives infectées. Connaître la date de l'attaque permet de ne traiter que les données transmises antérieurement à l'attaque. Une attention toute particulière doit être portée aux mandats et les **IBAN des bénéficiaires**. Les pièces justificatives pouvant être infectées, il ne faut pas les ouvrir.

> Stopper les accès des régisseurs au PIGP - compte créé par les services DFT

La gestion des utilisateurs et des habilitations incombe aux services Dépôts de Fond au Trésor (DFT) des directions locales pour l'ensemble des clients déposants. A ce titre et sur demande du mandataire sur le compte, les services DFT créent des identifiants dans ASPASIE et suivant les besoins autorisent l'accès à l'application de consultation de compte (DFT-Net) et/ou aux passerelles de télé-transmission pour dépôt/réception de fichiers de paiement.

Dans le cas d'une cyber-attaque, le service DFT de la direction locale doit être immédiatement informé. Suivant l'analyse et l'ampleur de l'attaque celui-ci pourra procéder à la coupure temporaire des accès aux comptes concernés en supprimant les habilitations Madrhas des utilisateurs associés aux comptes (suppression des REFCLI) ou en modifiant les mots de passe ASPASIE (après modification des adresses mails sur les comptes Aspasia).

Pour ne pas scléroser l'activité du client DFT et au cas par cas, le service DFT doit alors contacter la BALF DFT de la MAB mission.bancaire-dft@dgfip.finances.gouv.fr pour proposer des solutions alternatives.

Prévenir les interlocuteurs compétents au sein de la DGFiP

[Alerter

Chaque département organise la façon de déclarer l'incident aux services à compétence nationale. La désignation d'une personne référente cyber considérée comme coordinatrice des échanges est une bonne pratique. Il peut s'agir du responsable du SGC ou bien un membre de la direction locale (en fonction des organisations locales : Chef de division SPL, Directeur du pôle GP, responsable défense économique, MDRA).

La déclaration par mail doit être faite avec l'objet « **CYBER – ATTAQUE / Nom de la structure** » aux interlocuteurs ci dessous. Il est important de conserver la boucle des échanges en ne supprimant pas de destinataires au gré des réponses.

[Déclarer

La déclaration d'une attaque est à adresser aux différents bureaux ci dessous selon les indications de l'encadré bleu :

Bureau SI-3	Security Opération Center (Soc) et RSSI de la DGFiP
Bureau GP-2B	MOA en charge de l'application Hélios et coordination
Bureau GP-1A	Affaires juridiques
Mission RDCIC	Mission Responsabilité doctrine et contrôle interne comptable
Helios Flux 57	Gestion et supervision des flux à destination d'Hélios
Esi Châlons en Champagne	Gestion des échanges de flux via le PIGP

DESTINATAIRES DU MAIL

- **Pour aller plus vite, vous pouvez générer le mail d'alerte en cliquant sur ce lien : [déclaration d'une cyber-attaque](#).**
- **Si ce lien ne fonctionne pas, faites un copier coller des adresses :**
bureau.si3-dmocss@dgfip.finances.gouv.fr,soc@dgfip.finances.gouv.fr,bureau.gp2b-pes@dgfip.finances.gouv.fr,bureau.gp2b@dgfip.finances.gouv.fr,bureau.gp2b-demat-pj-cdg@dgfip.finances.gouv.fr,bureau.gp1a@dgfip.finances.gouv.fr,mission.rdcic-escroquerie@dgfip.finances.gouv.fr,helios.flux57@dgfip.finances.gouv.fr,esi.chalons.xfbgateway@dgfip.finances.gouv.fr

INFORMATIONS À DÉCLARER

- Codique du poste comptable
- Codes des budgets collectivités impactés par l'attaque
- Siret des budgets collectivités impactés par l'attaque
- Description de la détection de la cyber-attaque
- Description des logiciels impactés (Gestion financière, de facturation, de ressources humaines ...)
- Les fiches navettes (numéro de partenaire VPN)
- Liste des identifiants ASPASIE des personnes habilitées au portail PIGP.